REMARKS

I. Introduction

Claims 1-5 are pending in the above application.

Claim 1 stands rejected under 35 U.S.C. § 102.

Claims 2 and 3-5 stand rejected under 35 U.S.C. § 103.

Claims 1, 2 and 5 are independent claims.

II. Prior Art Rejections

A. Claim 1 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Yorke-Smith (U.S. Pat. 5,548,648).

Anticipation under 35 U.S.C. § 102 requires that each and every element of the claim be disclosed in a prior art reference as arranged in the claim. See, *Akzo N.V. v. U.S. Int'l Trade Commission*, 808 F.2d 1471 (Fed. Cir. 1986); *Connell v. Sears, Roebuck & Co.*, 220 USPQ 193, 198 (Fed. Cir. 1983).

As explained in Applicant's previous response submitted on March 30, 2005, Yorke-Smith does not disclose or suggest a method for encrypting information using encryption keys which uses a second key to encrypt a second portion of a message wherein the second portion overlaps with a first encrypted portion and also includes at least one bit of information in clear text, as recited by claim 1. Yorke-Smith merely discloses to divide a data string into a plurality of data segments DS, and to encrypt each data segment DS using a plurality of encryption techniques to obtain an encrypted data block EDS. Col. 3: 25-65. A control block CB is also provided which "comprises a plurality of fields containing information concerning the format of

the data bytes in the encrypted data block (EDB), in particular the encryption function (F) and encryption key (K) used to encrypt the data segment (DS)." Col. 3: 33-38. There is simply no discussion in Yorke-Smith which suggest to use a second key to encrypt a second portion of a message wherein the second portion overlaps with a first encrypted portion and also includes at least one bit of information in clear text, as recited by claim 1.

In response to the above explanation, the Office action alleges that Figure 3 and Col. 3, lines 1-15 "clearly describe that the encrypted block gets encrypted again with CB1 ...CBn, where CB comprises a plurality of fields containing information concerning the format of the data bytes in the encrypted data block EDB1 ... EDBn." Office action, pg. 6. The Examiner is respectfully mistaken. Nowhere does Yorke-Smith suggest to generate a data portion for encryption which "overlaps with a first encrypted portion," includes a second portion of the message, and includes at least one bit of information in the clear text. The Office action has not identified such in Yorke-Smith.

Moreover, CB is a control block, i.e., CB identifies the format of the data bytes, and identifies the encryption function F and encryption key K used to encrypt an associated data block. CB is not stated to be used as an encryption key or an encryption function, as the Office action seems to suggest. Col. 4: 1-15 of Yorke-Smith, cited to in the Office action, merely explains that several encryption functions F1 to Fi and several keys K1 to Kj may be selected from to encrypt a data segment, i.e. "different encryption functions and encryption keys selected from the range of available encryption functions (F1 to Fi) and encryption keys (K1 to Kj) are used to encrypt each data segment (DS1 to DSn) ... the encryption function used to encrypt a data segment is determined ...". Col. 3: 64 through Col. 4: 6. Figure 3 is merely illustrating the code after several data segments are encrypted, e.g., "when each data segment (DS1 to DSn) has

been encrypted the total encrypted code will comprise a plurality of encrypted data blocks (EDB1 to EDBn) and associated control blocks (CB1 to CBn) as illustrated in FIG. 3." Col. 4: 10-15.

Accordingly, Applicant respectfully requests the above rejection to be withdrawn.

B. Claims 2 and 3-5 stand rejected under 35 U.S.C. § 103 as being unpatentable over York-Smith in view of Koopman, Jr. et al. (U.S. Pat.5,619,575).

Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. *Ecolochem Inc. v. Southern California Edison Co.*, 227 F.3rd 1361, 56 U.S.P.Q.2d (BNA) 1065 (Fed. Cir. 2000); *In re Dembiczak*, 175 F.3d 994, 999, 50 U.S.P.Q.2D (BNA) 1614, 1617 (Fed. Cir. 1999); *In re Jones*, 958 F.2d 347, 21 U.S.P.Q.2d 1941 (Fed. Cir. 1992); and *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988). See also MPEP 2143.01.

Neither Yorke-Smith nor Koopman, taken alone or in combination, disclose or suggest a method for encrypting information in a message that can be authenticated which includes encrypting a second cipher subblock and the residual portion together with the second authentication block using a second key to form a cipher residual block, as substantially required by each of claims 2 and 5. Yorke-Smith does not disclose to encrypt a cipher subblock and a residual portion together with an authentication block. Yorke-Smith appears to only perform a single level of encryption, and clearly does not disclose to combine a portion of encrypted data with other data to be encrypted, and then encrypt. Koopman also does not disclose the above

features. Koopman appears to only disclose a pseudorandom cryptographic authentication process.

Accordingly, as neither Yorke-Smith nor Koopman, taken alone or in combination, disclose or suggest all of the limitations of the claims, the combination of Yorke-Smith and Koopman does not render claims 2 or 5 unpatentable. Likewise, as claims 3 and 4 depend on claim 2, and incorporate all of the limitations thereof, the combination of Yorke-Smith and Koopman does not render these claims unpatentable.

III. Conclusion

Having fully responded to the Office action, the application is believed to be in condition for allowance. Should any issues arise that prevent early allowance of the above application, the examiner is invited contact the undersigned to resolve such issues.

To the extent an extension of time is needed for consideration of this response, Applicant hereby request such extension and, the Commissioner is hereby authorized to charge deposit account number 502117 for any fees associated therewith.

Date: 3/1/06

Respectfully submitted,

By: _____

Lawrence T. Cullen
Reg. No.: 44,489

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
(215) 323-1797